AMENDMENT TO CLAIMS

1. (Currently amended) A network element having a plurality of features wherein at least one of the features may be optionally enabled or disabled, the network element comprising:

a service module that provides a first network features that may be optionally enabled or disabled;

a system processor that is operable to receive a softkey value inputted from outside of the network element, wherein the softkey value is received by the network element via a network connection; and

a softkey validation system that is operable to enable the use of the first network feature when the received softkey value is the same as a first valid softkey value, the softkey validation system also being operable to enable the use of the first network feature a second time, after the first network feature has been deactivated, when the received softkey value is the same as a second valid softkey value, wherein the first valid softkey value is not the same as the second valid softkey value and the first and the second softkey values are machine generated and can be used only once in relation to the first network feature, the softkey validation system comprising:

memory for storing information related to the service module; and

an algorithm, wherein said softkey validation system when executing said algorithm is operable to confirm for use in confirming whether the received softkey value is a valid softkey value; and

wherein upon confirmation that the received softkey value is valid the softkey validation system enables the use of the network feature.

2. (Original) The network element according to claim 1 wherein enabling the use of the network feature comprises enabling the use of the network feature without the generation of alarms.

3.   (Original) The network element according to claim 1 wherein enabling the use of the network

feature comprises enabling the use of the network feature when the network feature could not be

used, even in an alarm state, without being enabled through the softkey system.

4.   (Original) The network element according to claim 1 wherein the algorithm is operable for

generating a deactivated softkey value when the first network feature has been deactivated.

5.   (Currently amended) A node element in a communication network, comprising:

a service module that provides a first network features that may be optionally enabled or

disabled;

a system processor that is operable to receive a softkey value inputted from outside of the

network element wherein the softkey value is received by the network element via a network

connection; and

a softkey validation system that is operable to enable the use of the first network feature

when the received softkey value is the same as a first valid softkey value, the softkey validation

system also being operable to enable the use of the first network feature a second time, after the first

network feature has been deactivated, when the received softkey value is the same as a second valid

softkey value, wherein the first valid softkey value is not the same as the second valid softkey value

and the first and the second softkey values are machine generated and can be used only once in

relation to the first network feature, the softkey validation system comprising:

memory for storing information related to the service module; and

an algorithm, wherein said softkey validation system when executing said algorithm

is operable to confirm for use in confirming whether the received softkey value is a valid softkey

value; and

wherein upon confirmation that the received softkey value is valid the softkey system enables the use of the network feature.

6. (Original) The node element according to claim 5 wherein the service module is a communication module.

7. (Original) The node element according to claim 5 wherein the first network feature is a communication port.

8. (Original) The node element according to claim 7 wherein the first network feature is a OC-3 port.

9. (Original) The node element according to claim 7 wherein the first network feature is a OC-12 port.

10. (Original) The node element according to claim 7 wherein the first network feature is a OC-48 port.

11. (Original) The node element according to claim 7 wherein the first network feature is a OC-192 port.

12. (Original) The node element according to claim 7 wherein the first network feature is a EC-1 port.

13. (Original) The node element according to claim 7 wherein the first network feature is a DS3 port.

14. (Original) The node element according to claim 7 wherein the first network feature is a DS1 port.

15. (Original) The node element according to claim 7 wherein the first network feature is a E1 port.

CLI-1327932v1   4

16. (Original) The node element according to claim 7 wherein the first network feature is an Ethernet port.

17. (Original) The node element according to claim 7 wherein the first network feature is a Fast Ethernet port.

18. (Original) The node element according to claim 7 wherein the first network feature is a Gigabit Ethernet port.

19. (Original) The node element according to claim 5 wherein the service module is an optical mapper.

20. (Original) The node element according to claim 19 wherein the first network feature is an optical network port.

21. (Currently amended) The node element according to claim 5 wherein the service module is implemented in a form of a software program stored in said node element.

22. (Currently amended) The node element according to claim 21 wherein the first network feature is an output from the software program when the software program is executed on said node element.

23. (Currently amended) A system for enabling the use of network features in a network element, comprising:

a softkey assignment system that is operable to perform operations with respect to at least one softkey, the softkey assignment system being operable to assign a softkey value to the softkey and to update the softkey status to an assigned state upon the assignment of a softkey value to the softkey, the softkey assignment system also being operable to update the softkey status to an unassigned state upon the receipt of a deactivate softkey value for the softkey; and

a network element, the network element comprising:

a service module that provides a first network features that may be optionally

enabled or disabled; and

a system processor that is operable to receive a softkey value inputted from outside

of the network element, wherein the softkey value is received by the network element via a network

connection; and

a softkey validation system that is operable to enable the use of the first network

feature when a received softkey value is the same as a first valid softkey value, the softkey

validation system also being operable to enable the use of the first network feature a second time,

after the first network feature has been deactivated, when the received softkey value is the same as a

second valid softkey value, wherein the first valid softkey value is not the same as the second valid

softkey value and the first and the second softkey values are machine generated and can be used

only once in relation to the first network feature.

24.   (Original) The system according to claim 23 wherein the service module includes the softkey

validation system.

25.   (Original) The system according to claim 23 wherein the network element further comprises a

shelf processor and wherein the shelf processor includes the softkey validation system.

26.   (Original) The system according to claim 23 wherein the service module comprises an

internal counter and wherein the internal counter stores a value that is used by the softkey

validation system in determining whether the received softkey value is valid.

27.   (Currently amended) A method for enabling the use of network features in a network element

within a network, the network element comprising a service module that provides a first network

features that may be optionally enabled, the method comprising the steps of:

receiving an encrypted softkey value from outside of the network element, wherein the softkey value is received by the network element via a network connection;

decrypting the encrypted softkey value;

determining whether the received softkey value is equal to a first valid softkey value;

enabling the first network feature if the received softkey value is equal to the first valid softkey value; and

providing a mechanism for deriving a second valid softkey value wherein the second valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be activated if the first network feature is deactivated after it has been activated using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be activated again if the first network feature is deactivated after it has been activated using the first valid softkey value and the first and the second softkey values are machine generated and can be used only once in relation to the first network feature.

28. (Currently amended) A method for enabling the use of network features in a network, the network comprising a softkey assignment system, and a network element comprising a service module that provides a first network features that may be optionally enabled, the method comprising the steps of:

providing a customer with a reusable softkey;

generating with the softkey assignment system a softkey value for the softkey;

encrypting the softkey value;

assigning the encrypted softkey value to the softkey;

providing the encrypted softkey value to the customer upon the customer's request to use the softkey;

updating the state of the softkey to an assigned state upon assigning the encrypted softkey value to the softkey;

providing within the network element a validation system that is operable to: (a) receive an encrypted softkey value from outside of the network element, wherein the softkey value is received by the network element via a network connection, (b) decrypt the encrypted softkey value, (c) determine whether the received softkey value is equal to a first valid softkey value, and (d) enable the first network feature if the received softkey value is equal to the first valid softkey value;

providing with the service module a system for deriving a second valid softkey value wherein the second valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be activated if the first network feature is deactivated after it has been activated using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be activated again if the first network feature is deactivated after it has been activated using the first valid softkey value and the first and the second softkey values are machine generated and can be used only once in relation to the first network feature;

providing a method for allowing the customer to return the softkey to an unassigned state; and

allowing the customer to re-use the softkey for activating a second network feature by allowing the softkey assignment system to provide the customer with a second softkey value upon request if the softkey is in an unassigned state at the time of the request.

CLI-1327932v1   8

29. (Original) The method of claim 28 wherein the providing a method for allowing the customer to return the softkey step comprises the steps of:

provicling within the network element a system for deactivating the feature associated with the installed softkey and for returning to the customer a deactivation key value upon deactivation of the feature;

accepting the deactivation key value from the customer; and

updating the state of the softkey to reflect that it is in an unassigned state.

30. (Original) The method of claim 28 wherein the system for deriving a second valid softkey value comprises a counter within the service module that keeps track of the number of times that the service module feature has been activated.

31. (Original) The method of claim 28 wherein the system for deriving a second valid softkey value comprises a counter within the service module that keeps track of the number of times that the service module feature has been activated.

32. (Original) The method of claim 28 wherein the service module comprises a key holding location and wherein the first network feature is enabled by loading a valid key value into the key holding location.

33. (Original) The method of claim 28 wherein the service module comprises a key holding location and wherein the first network feature is enabled by loading data derived from at least a portion of the valid key value into the key holding location.

34. (Currently amended) A method for authorizing the use of a network feature in a network, the network comprising a softkey assignment system, and a network element comprising a service module that provides a first network feature that may be optionally authorized, the method comprising the steps of:

allowing a customer to use the first network feature;

generating an alarm condition when the customer uses the first network feature without supplying a softkey value;

providing a customer with a softkey upon request by the customer;

generating the softkey value for the softkey;

providing the softkey value to the customer upon request by the customer; and

canceling the alarm condition in response to the customer supplying the softkey value to the network element, wherein the softkey value is encrypted and wherein the network element comprises a validation system that is operable to: (a) receive the encrypted softkey value from outside of the network element, wherein the softkey value is received by the network element via a network connection, (b) decrypt the encrypted softkey value, (c) determine whether the received softkey value is equal to a first valid softkey value, and (d) authorize the use of the first network feature if the received softkey value is equal to the first valid softkey value; and

wherein the service module comprises a system for deriving a second valid softkey value wherein the second valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be authorized if the first network feature is de-authorized after it has been authorized using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be authorized again if the first network feature is de-authorized after it has been authorized using the first valid softkey value and the first and the second softkey values are machine generated and can be used only once in relation to the first network feature.

Claims 35 - 36 (Cancelled).